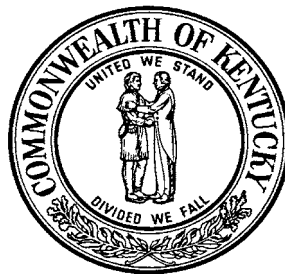


**LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
CABINET FOR HEALTH SERVICES**

**In Reference to the Statewide Single Audit
of the Commonwealth of Kentucky**

For the Year Ended June 30, 2002



EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS
www.kyauditor.net

**144 CAPITOL ANNEX
FRANKFORT, KY 40601
TELEPHONE (502) 564-5841
FACSIMILE (502) 564-2912**

CONTENTS

MANAGEMENT LETTER	1
LIST OF ABBREVIATIONS/ACRONYMS	3
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS.....	10
FINANCIAL STATEMENT FINDINGS	13
<i>Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance</i>	<i>13</i>
FINDING 02-CHS-1: The Cabinet For Health Services Should Strengthen The Security Of System Administrator Accounts	13
FINDING 02-CHS-2: The Vital Statistics Branch Should Improve Controls Over Assets And Separate Work Tasks.....	15
FINDING 02-CHS-3: The Vital Statistics Branch Should Take Appropriate Steps To Reduce The Identity Theft Risks	21
<i>Other Matters Relating to Internal Controls and/or Reportable Instances of Noncompliance</i>	<i>23</i>
FINDING 02-CHS-4: The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized.....	23
FINDING 02-CHS-5: The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose	25
FINDING 02-CHS-6: The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers	27
FINDING 02-CHS-7: The Cabinet For Health Services Should Remove The Simple Network Management Protocol Service Or Change The Default Community String.....	29
FINDING 02-CHS-8: The Cabinet For Health Services Should Ensure All User Accounts On Its Agency Servers Are Necessary	30
FINDING 02-CHS-9: The Vital Statistics Branch Has An Outdated Computer System	32
FINDING 02-CHS-10: Vital Statistics Policies And Procedures Should Be Upgraded	33
FINDING 02-CHS-11: The Timesheet Preparation Process Needs Better Oversight.....	34

CONTENTS

<i>Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance</i>	<i>35</i>
FINDING 02-CHS-12: The Division Of Program Integrity Has A Large Outstanding Balance Of Accounts Receivable For The Drug Rebate Program.....	35
FINDING 02-CHS-13: The Division Of Program Integrity Does Not Track Interest Due On Outstanding Drug Rebate Accounts.....	37
FINDING 02-CHS-14: The Division Of Managed Care Does Not Maintain Records Of Complaints And Grievances	39
<i>Other Matters Relating to Internal Controls and/or Compliance.....</i>	<i>41</i>
FINDING 02-CHS-15: The Division Of Systems And Member Services Does Not Reconcile Supplementary Insurance Billing.....	41
FINDING 02-CHS-16: The Office Of Aging Does Not Document The Performance Of Desk Reviews.....	43
FINDING 02-CHS-17: The Office Of Aging Did Not Make Monitoring Visits To All Area Agencies	44
SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS	45



EDWARD B. HATCHETT, JR.
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Paul E. Patton, Governor
Marcia Morgan, Secretary
Cabinet for Health Services

MANAGEMENT LETTER

This letter presents the results of our audit of the Cabinet for Health Services, performed as part of our annual Statewide Single Audit of the Commonwealth of Kentucky.

In planning and performing our audit of the financial statements of the Commonwealth for the year ended June 30, 2002, we considered the Cabinet for Health Services' internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. We also performed an audit on compliance with requirements applicable to major federal programs, as well as the Schedule of Expenditures of Federal Awards. We noted certain matters involving internal control, compliance and its operation that we are including in this letter. Some findings are considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants.

Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control and compliance that, in our judgment, could adversely affect the Cabinet for Health Services' ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. Reportable conditions could also adversely affect the Cabinet for Health Services' ability to administer a major federal program in accordance with the applicable requirements of laws, regulations, contracts, and grants.

A material weakness is a reportable condition in which the design or operation of one or more internal control components does not reduce to a relatively low level the risk that errors or irregularities in amounts that would be material in relation to the financial statements or federal programs being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions.

Our consideration of the internal control would not necessarily disclose all matters in the internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses as defined above. However, none of the reportable conditions described herein is believed to be a material weakness.



To the People of Kentucky
Honorable Paul E. Patton, Governor
Marcia Morgan, Secretary
Cabinet for Health Services

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with Government Auditing Standards.

Included in this letter are the following:

- ◆ Acronym List
- ◆ Schedule of Expenditures of Federal Awards
- ◆ Notes to the Schedule of Expenditures of Federal Awards
- ◆ Findings (Reportable, Material, and Other Matters)
- ◆ Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains the Cabinet for Health Services' findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.kyauditor.net.

This letter is intended solely for the information and use of management and federal awarding agencies and pass-through entities and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Ed Hatchett", with a long horizontal flourish extending to the right.

Edward B. Hatchett, Jr.
Auditor of Public Accounts

LIST OF ABBREVIATIONS/ACRONYMS

ADD	Area Development Districts
APA	Auditor of Public Accounts
BDC	Backup Domain Controllers
CFDA	Catalog of Federal Domestic Assistance
CHR	Cabinet for Human Resources (former name of the Cabinet for Health Services and the Cabinet for Families and Children)
CIM	Compaq Insight Manager
CMS	Center for Medicare and Medicaid Services
CHS	Cabinet for Health Services
DHHS	Department of Health and Human Services
DMS	Department of Medicaid Services
DSI	Department of Social Insurance
DTR	Division of Technology Resources
FAC	Finance and Administrative Cabinet
FMRB	Financial Management and Reporting Branch
FTP	File Transfer Protocol
FY	Fiscal Year
HIPPA	Health Insurance Privacy and Portability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
KAR	Kentucky Administrative Regulations
KRS	Kentucky Revised Statutes
LAN	Local Area Network
LHD	Local Health Department
LSA	Local Security Authority
MAID	Medical Assistance Identification
MARS	Management Administrative and Reporting System
MMIS	Medicaid Management Information System
NAPHSIS	National Association for Public Health Statistics and Information Systems
NA	Not Applicable
NDC	National Drug Code
NT	New Technology (Microsoft Windows operating system)
OBRA	Omnibus Budget Reconciliation Act
OAG	Office of Attorney General
OAS	Office of Aging Services
OMB	Office of Management and Budget
PC	Personal Computer
PDC	Primary Domain Controller
QCSI	Quality Care Solutions, Inc.
R&D	Research and Development
RCW	Record of Control Weakness
SAS	Statements on Auditing Standards
SMI	Supplementary Medical Insurance
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
U.S	United States
VAX	Virtual Address extension
VSIS	Vital Statistics Information System

**SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002**

CFDA #	Program Title	Expenditures		Provided to Subrecipient
		Cash	Noncash	
<u>U.S. Department of Agriculture</u>				
Direct Programs:				
10.557	Special Supplemental Program for Women, Infants and Children	\$ 82,607,353	\$	\$ 16,214,985
10.570	Nutrition Services Incentive	2,573,718		2,573,718
Passed Through From Cabinet for Families and Children:				
10.561	State Administrative Matching Grants for Food Stamp Program	191,725		
<u>U.S. Department of Labor</u>				
Direct Program:				
17.235	Senior Community Service Employment Program	1,666,319		1,615,886
Passed Through From Cabinet for Families and Children:				
17.253	Welfare-to-Work Grants to States and Localities	205		
<u>U.S. Department of Transportation</u>				
Passed Through From Kentucky State Police				
20.600	State and Community Highway Safety	74,956		
<u>U.S. Environmental Protection Agency</u>				
Direct Programs:				
66.032	State Indoor Radon Grants	195,513		129,849
66.606	Surveys, Studies, Investigations and Special Purpose Grants	159,134		1,883
66.707	TSCA Title IV State Lead Grants - Certification of Lead-Based Paint Professionals	281,957		
<u>U.S. Department of Energy</u>				
Direct Program:				
81.106	Transport of Transuranic Wastes to the Waste Isolation Pilot Plant: States and Tribal Concerns, Proposed Solutions	22,043		

**SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002**

CFDA #	Program Title	Expenditures		Provided to Subrecipient
		Cash	Noncash	
<u>U.S. Department of Energy (Continued)</u>				
Passed Through From the Cabinet for Families and Children				
81.042	Weatherization Assistance for Low-Income Persons	96,374		
Passed Through From Natural Resources				
81.502	Department of Energy	389,371		112,536
<u>U.S. Federal Emergency Management Agency</u>				
Passed Through From Military Affairs				
83.549	Chemical Stockpile Emergency Preparedness Program	140,145		76,610
<u>U.S. Department of Education</u>				
Direct Programs:				
84.181	Special Education -- Grants for Infants and Families with Disabilities	2,514,688		579,039
84.186	Safe and Drug-Free Schools and Communities -- State Grants	1,212,864		1,212,863
Passed Through From Department of Education				
84.323	Special Education -- State Program Improvement Grants for Children with Disabilities	63,818		36,077
<u>U.S. Department of Health and Human Services</u>				
Direct Programs:				
93.003	Public Health and Social Services Emergency Fund	100,000		
93.041	Special Programs for the Aging -- Title VII, Chapter 3 -- Programs for Prevention of Elder Abuse, Neglect, and Exploitation	65,760		65,760
93.042	Special Programs for the Aging -- Title VII, Chapter 2 -- Long-term Care Ombudsman Services for Older Individuals	120,264		51,035
93.043	Special Programs for the Aging -- Title III, Part D -- Disease Prevention and Health Promotion Services	316,075		313,746

**SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002**

CFDA #	Program Title	Expenditures		Provided to
		Cash	Noncash	Subrecipient
<u>U.S. Department of Health and Human Services (Continued)</u>				
Direct Programs (Continued):				
Aging Cluster:				
93.044	Special Programs for the Aging -- Title III, Part B -- Grants for Supportive Services and Senior Centers (Note 2)	4,970,611		4,719,861
93.045	Special Programs for the Aging -- Title III, Part C -- Nutrition Services (Note 2)	7,327,533		6,964,340
93.046	Special Programs for the Aging – Title III, Part D – In-Home Services for Frail Older Individuals	43,527		
93.048	Special Programs for the Aging -- Title VI and Title II -- Discretionary Projects	13,785		13,785
93.052	National Family Caregiver Program	1,232,759		1,165,419
93.103	Food and Drug Administration -- Research	4,000		
93.104	Comprehensive Community Mental Health Services for Children with Serious Emotional Disturbances (SED)	1,565,793		1,564,550
93.110	Maternal and Child Health Federal Consolidated Programs (Note 3)	179,457		
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs (Note 3)	1,014,425	80,905	814,578
93.119	Grants for Technical Assistance Activities Related to the Block Grant for Community Mental Health Services - Technical Assistance Centers for Evaluation	59,228		59,228
93.130	Primary Care Services – Resource Coordination and Development	77,044		53,175
93.136	Injury Prevention and Control Research and State and Community Based Programs	617,918		617,918
93.150	Projects for Assistance in Transition from Homelessness (PATH)	300,000		300,000
93.197	Childhood Lead Poisoning Prevention Projects – State and Local Childhood Lead Poisoning Prevention and Surveillance of Blood Levels in Children	137,902		
93.217	Family Planning - Services	4,675,493		4,484,717
93.230	Consolidated Knowledge Development and Application (KD&A) Program (Note 4)	3,405,317		3,405,317
93.235	Abstinence Education	1,050,177		998,135
93.238	Cooperative Agreements for State Treatment Outcomes and Performance Pilot Studies Enhancement (Note 4)	392,556		330,285
93.262	Occupational Safety and Health Research Grants	61,560		61,560
93.268	Immunization Grants (Note 3)	2,902,603	11,697,542	1,874,493
93.283	Centers for Disease Control and Prevention – Investigations and Technical Assistance	2,469,006		2,085,218
93.630	Developmental Disabilities Basic Support and Advocacy Grants	1,158,051		557,608

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002**

CFDA #	Program Title	Expenditures		Provided to Subrecipient
		Cash	Noncash	
<u>U.S. Department of Health and Human Services (Continued)</u>				
Direct Programs (Continued):				
93.767	State Children’s Insurance Program (Note 2)	59,841,382		412,280
Medicaid Cluster:				
93.777	State Survey and Certification of Health Care Providers and Suppliers (Note 2)	5,206,307		
93.778	Medical Assistance Program (Note 2)	2,647,415,374		2,899,984
93.779	Centers for Medicare and Medicaid Services (CMS) Research, Demonstrations and Evaluations	483,578		412,244
93.917	HIV Care Formula Grants	5,896,036		4,700,591
93.919	Cooperative Agreements for State-Based Comprehensive Breast and Cervical Cancer Early Detection Programs	2,436,871		2,135,516
93.940	HIV Prevention Activities – Health Department Based (Note 3)	2,077,367	38,436	1,666,647
93.944	Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Virus Syndrome (AIDS) Surveillance	126,933		85,413
93.945	Assistance Programs for Chronic Disease Prevention and Control	650,751		300,949
93.958	Block Grants for Community Mental Health Services	5,178,274		5,171,313
93.959	Block Grants for Prevention and Treatment of Substance Abuse (Note 2)	19,213,490		18,581,135
93.977	Preventive Health Services – Sexually Transmitted Diseases Control Grants (Note 3)	770,045	354,304	171,131
93.988	Cooperative Agreements for State-Based Diabetes Control Programs and Evaluation of Surveillance Systems	410,365		309,558
93.991	Preventive Health and Health Services Block Grant	2,401,053		2,264,727
93.994	Maternal and Child Health Services Block Grant to the States (Note 3)	8,046,928		7,994,367
Passed Through From Cabinet for Families and Children				
93.556	Promoting Safe and Stable Families (Note 2)	1,577		
93.558	Temporary Assistance for Needy Families (Note 2)	220,669		
93.563	Child Support Enforcement (Note 2)	15,042		
93.568	Low-Income Home Energy Assistance (Note 2)	15,037		
93.569	Community Services Block Grant (Note 2)	16,502		
93.596	Child Care Mandatory and Matching Funds of the Child Care and Development Fund (Note 2)	2,328,613		
93.658	Foster Care – Title IV E (Note 2)	109,196		

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002**

CFDA #	Program Title	Expenditures		Provided to
		Cash	Noncash	Subrecipient
<u>U.S. Department of Health and Human Services (continued)</u>				
Passed Through From Cabinet for Families and Children (Continued)				
93.667	Social Services Block Grant (Note 2)	140,627		125,755
93.669	Child Abuse and Neglect State Grants (Note 2)	119		
93.671	Shelters – Grants to States and Indian Tribes (Note 2)	3,406		
93.674	Chafee Foster Care Independent Living (Note 2)	11		
NA	Chemical Laboratory Improvement Act (Note 3)	188,100		
<u>U.S. Corporation for National and Community Service</u>				
Direct Program:				
94.011	Foster Grandparent Program	469,388		75,442
TOTAL CABINET FOR HEALTH SERVICES		\$2,890,114,068	\$12,171,187	\$100,361,226

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002

Note 1 - Purpose of the Schedule and Significant Accounting Policies

Basis of Presentation - OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, requires a Schedule of Expenditures of Federal Awards showing each federal financial assistance program as identified in the *Catalog of Federal Domestic Assistance*. The accompanying schedule includes all federal grant activity for the Commonwealth, except those programs administered by state universities, and is presented primarily on the basis of cash disbursements as modified by the application of Kentucky Revised Statute (KRS) 45.229. Consequently, certain expenditures are recorded in the accounts only when cash is disbursed. The Commonwealth elected to exclude state universities from the statewide single audit, except as part of the audit of the basic financial statements.

KRS 45.229 provides that the Finance and Administration Cabinet may, “for a period of thirty (30) days after the close of any fiscal year, draw warrants against the available balances of appropriations made for that fiscal year, for the payment of expenditures incurred during that year or in fulfillment of contracts properly made during the year, but for no other purpose.” However, there is an exception to the application of KRS 45.229 in that regular payroll expenses incurred during the last pay period of the fiscal year are charged to the next year.

The basic financial statements of the Commonwealth are presented on the modified accrual basis of accounting for the governmental fund financial statements and the accrual basis of accounting for the government-wide, proprietary fund, and fiduciary fund financial statements. Therefore, the schedule may not be directly traceable to the basic financial statements in all cases.

Noncash assistance programs, where applicable, are not reported in the basic financial statements of the Commonwealth for FY 02. The noncash expenditures presented on this schedule represent the noncash assistance expended using the method or basis of valuation described in Note 13.

Clusters of programs are indicated in the schedule by light gray shading.

Inter-Agency Activity - Certain transactions relating to federal financial assistance may appear in the records of more than one (1) state agency. To avoid the overstatement of federal expenditures, the following policies were adopted for the presentation of the schedule:

- (a) Federal moneys may be received by a state agency and passed through to another state agency where the moneys are expended. Except for pass-throughs to state universities as discussed below, this inter-agency transfer activity is reported by the agency expending the moneys.

State agencies that pass federal funds to state universities report those amounts as expenditures.

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002

Note 1 - Purpose of the Schedule and Significant Accounting Policies (Continued)

Inter-Agency Activity (Continued)

- (b) Federal moneys received by a state agency and used to purchase goods or services from another state agency are reported in the schedule as an expenditure by the purchasing agency only.

Note 2 - Type A Program

Type A programs for the Commonwealth mean any program for which total expenditures of federal awards exceeded \$17 million for FY 02. The Cabinet for Health Services had the following programs that met Type A program definition for FY 02. Clusters are identified by gray shading.

CFDA #	Program Title	Expenditures
93.959	Block Grants for Prevention and Treatment of Substance Abuse	\$ 19,213,490
93.767	State Children's Health Insurance Program	59,841,382
Medicaid Cluster:		
93.777	State Survey And Certification Of Health Care Providers And Suppliers	5,206,307
93.778	Medical Assistance Program	2,647,415,374
Total Type A Programs		<u>\$2,743,974,697</u>

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2002

Note 3 - Noncash Expenditure Programs

The Cabinet for Health Services had four noncash programs for the year ended June 30, 2002. These noncash programs and a description of the method/basis of valuation follow:

CFDA #	Program Title	Amount	Method/Basis of Valuation
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs	\$ 80,905	Per authorized award for personnel costs and travel.
93.268	Immunization Grants	11,697,542	Per authorized award for personnel, vaccine costs, and travel.
93.940	HIV Prevention Activities - Health Department Based	38,436	Per authorized award for personnel costs.
93.977	Preventive Health Services - Sexually Transmitted Diseases Control Grants	354,304	Per authorized award for personnel and travel.
Total Noncash Expenditures		<u>\$12,171,187</u>	

Note 4 - Research and Development Expenditures

OMB Circular A-133 Section 105 states, "Research and development (R&D) means all research activities, both basic and applied, and all development activities that are performed by a non-Federal entity."

The expenditures presented in the SEFA include R&D expenditures. The R&D portion of the expenditures for each program is listed below.

CFDA #	Program Title	Expenditures
93.230	Consolidated Knowledge Development and Application (KD&A) Program	\$ 390,817
93.238	Cooperative Agreements for State Treatment Outcomes and Performance Pilot Studies Enhancement	228,119
		<u>\$ 624,056</u>

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-1: The Cabinet For Health Services Should Strengthen The
Security Of System Administrator Accounts**

Vulnerability testing of Cabinet for Health Services (CHS) servers revealed several instances of lax security over system Administrator accounts resulting in the potential of servers being vulnerable to intrusion.

We examined 33 CHS servers that provided NetBIOS information and found the system Administrator account for 12 servers, or 36 percent, had not been renamed or disabled. Since the Administrator cannot be locked out, if the account is not renamed, the server could be vulnerable to an intruder attempting to gain system access by guessing the Administrator password through a brute force attack.

Further, we examined the CHS servers for specific application vulnerabilities and found 15 machines with port 1433 open. Eight (8) servers allowed the auditor to gain "Master" access through SQL using the default administrator logon. This type of access would provide an unauthorized user with complete access to the application. In addition, the user would be granted local system account rights to the server on which the application resides. At the time of writing this comment all but one of these servers had been changed to prohibit access to SQL through the default logon.

Administrator accounts are very powerful and can allow full access to the system. To ensure that these accounts are adequately secured, passwords should be changed from the system defaults. Further, some Administrator accounts can be renamed to help obscure them from an unauthorized user's view.

Recommendation

We recommend that CHS review all servers to ensure the system Administrator accounts have been changed from the default-naming conventions and require the use of a password. Further, all applications that might allow a user access to the system or to configuration settings should be reviewed to ensure default logons are not allowed.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-1: The Cabinet For Health Services Should Strengthen The
Security Of System Administrator Accounts (Continued)**

Management's Response and Corrective Action Plan

CHS concurs with the recommendation of the APA and implemented corrective actions, effective September 2002, requiring system administrator accounts within the CHS domain to be renamed. The Division of Technology Resources (DTR) will conduct periodic internal audits, effective January 2003, to ascertain compliance with this recommendation.

Effective December 2002, DTR implemented a policy requiring server administrator passwords to be complex and to establish periodic testing and updates.

The DTR established administrator passwords on all MSSQL databases in CHS in July 2002. To reinforce this security vulnerability, the DTR created, in October 2002, a Cabinet policy indicating that no software applications were to be installed on any desktop machines except by experienced and authorized information technology personnel.

Effective January 2003, DTR will:

- Complete it's audit of administrator accounts and passwords.*
- Report to CHS executive staff regarding the need to educate staff on the policy in effect regarding no unauthorized installation of computer applications.*
- Include an article of in the CHS Checkup newsletter to inform staff on the presence of the policy regarding installation of computer applications.*
- Increase the frequency of network audits conducted by DTR in order to validate compliance with this Cabinet policy.*

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-2: The Vital Statistics Branch Should Improve Controls Over Assets And Separate Work Tasks**

The Vital Statistics Branch issues birth, death, marriage, and divorce certificates. Fees for these certificates are received from walk-in, mail, and phone requests. Due to two (2) instances of fraud during FY 00, the APA has given closer attention to the Vital Statistics Branch. We noted the following control weaknesses:

- 1) As reported in the two (2) previous audits, deposits were left unattended for inappropriate periods of time. This process, while somewhat improved, remains inadequate.
- 2) Certificates that must be voided are not retained and all procedures for the voiding of certificates are not properly segregated among employees. Because voided certificates are not retained, it is impossible to verify that the certificates were truly voided.
- 3) The rear entrance of the office does not have a door and thus non-branch employees can access areas where cash, checks, certificates, and vouchers are located. Unrestricted access through the rear door places these items at risk.
- 4) Certificate requests constitute most of the incoming mail of the branch. Mail and cash handling procedures implemented during this audit period are not adequate because the data entry operator performs all processing involved with each order received by mail. Data entry clerks, therefore, have the opportunity to misappropriate funds or misdirect information.
- 5) Funeral homes may obtain death certificates through the use of prepaid vouchers. We previously commented that the vouchers are easily counterfeited. Attempts by CHS to rectify this issue have not been successful. Also, there is a significant lack of duty segregation regarding the receipt and issuance of prepaid vouchers. This lack of segregation of duties places the payments for vouchers at risk.
- 6) Due to a lengthy receipts reconciliation process, receipts collected on one (1) business day are not deposited until two (2) business days later. KRS 41.070 (1) requires the timely deposit of public money. Delays in processing deposits increase the risk of funds being lost or stolen and deny the Commonwealth of additional interest earnings.
- 7) Documents containing citizen credit card information are not maintained in a secure manner during the workday.
- 8) Reports are run at the end of the day detailing the activity of each clerk. An Accountant III reviews the daily reports for errors, prepares the daily reconciliation, and prepares the daily deposit. This lack of segregation of duties places these receipts in jeopardy.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS2: The Vital Statistics Branch Should Improve Controls Over
Assets And Separate Work Tasks (Continued)**

- 9) The Vital Statistics Branch collects fees for certificates from walk-in traffic at the front desk. Receipts are not usually issued for cash payments. The chance of lost or stolen cash is greater without establishing proper controls.
- 10) The safe, in which blank death certificates are maintained, is left unlocked for excessive periods of time thus creating the potential for theft.
- 11) The branch maintains a supply of signed blank checks and these checks are properly stored in a locked safe. However, there is no reconciliation process in place, which would allow the branch to determine if all checks were properly accounted for. This lack of control places these checks at risk of being used fraudulently.

Recommendation

We recommend the following:

- 1) The Vital Statistics Branch provide better physical security over receipts. In the event of the Accountant III's absence, the branch supervisor should prepare the deposit.
- 2) The branch should have the document custodian maintain all voided certificates. In addition, someone other than the document custodian should void the certificates prior to being logged.
- 3) Install a door at the rear entrance, and the door should lock as it is shut. Only branch personnel should have access to this area.
- 4) The branch should segregate mail processing and data entry duties. A mail clerk or processor could open mail and log the contents of the correspondence—tracking requests, methods of payment, and amounts of payment. Requests should then be forwarded to data entry clerks for processing.
- 5) The branch should assign one (1) employee to be in charge of receiving the prepaid voucher money. Another employee should issue the vouchers.
- 6) The Vital Statistics Branch should deposit all receipts no later than the next business day after receiving them.
- 7) The branch should assess whether it is necessary to keep the entire fax order for possible verification of receipt of that order. If it is determined it is necessary to keep the orders, the branch should place them in a locked file.
- 8) The end-of-the day reconciliation function should be segregated from the deposit preparation function.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS2: The Vital Statistics Branch Should Improve Controls Over
Assets And Separate Work Tasks (Continued)**

Recommendation (Continued)

- 9) Vital Statistics Branch should issue pre-numbered receipts (manual or numbered cash register receipt) for all walk-in cash transactions. The cash register tape and the manual cash receipts should be batched and reconciled to the cash register reconciliation sheet.
- 10) The safe should only be opened by authorized personnel and should be closed and locked when not in use.
- 11) The branch should maintain an inventory log of all signed blank checks. The inventory should be reconciled two (2) to three (3) times a week.

Management's Response and Corrective Action Plan

- 1.) *The Vital Statistics Branch feels its policies and procedures for the physical security of receipts is adequate, this was an isolated incident. It is already procedure that when the Accountant III is not present to prepare the daily deposit it is the responsibility of the Fee Control Unit Supervisor, then the Accountant I, then a specified data entry operator. On the above day mentioned, all were absent but the data entry operator. All employees have again been counseled concerning the leaving of deposits unattended or unlocked, for any period of time.*
- 2.) *We are confused by the weakness mentioned in this audit comment. The current procedure in place is that if a void is necessary, the operator responsible stamps the certificate void and enters it on a log at his or her desk. The supervisor does not void the certificate. At the end of the day the supervisor crosschecks the voids with the operator's log. This is what we interpret this audit comment is asking along with the keeping of voids. Concerning the keeping of voids - the National Association for Public Health Statistics and Information Systems (NAPHSIS) published updated (9-10-02) standards for the establishment of internal policies and procedures for the handling of security paper. These standards were set by the NAPHSIS Fraud Committee and recommend that all states that use security paper to establish written policies and procedures including these recommendations. These standards recommend against the request by auditors that voids be logged and kept. The standard (Item 7) recommends voids being logged and crosschecked by a supervisor and destroyed. This procedure is currently in place. This office is not equipped to handle Item 6 that specifies all printing should be done in a single location although all printing is done within view of a supervisor. Effective November 2002, this*

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS2: The Vital Statistics Branch Should Improve Controls Over
Assets And Separate Work Tasks (Continued)**

Management's Response and Corrective Action Plan (Continued)

office will implement the recommendations that two authorized personnel are present when the safety paper is removed from the Vault security room and also the safes housing the paper on the first floor and that the logs contain a column for witness' initials; and that a log is placed at each printer (copier) for the operators (instead of at their desks as we now do).

- 3.) *The Finance Cabinet created a personnel access security program in the CHR Building to eliminate or minimize unauthorized entry to the building complex. As a result, only authorized personnel enter through either the front or rear door of Vital Statistics. The rope system is an added method of controlling entry to the Vitals area. Based on this initiative, reasonable risk management has been established.*

Current procedures control receipt, storage, retrieval and processing of pilferable assets. Access is reasonably controlled. As a result, to request construction funds to add doors (especially in the current environment) where no tangible decrease in asset risk can be quantified would not be prudent. In fact, the only recently recorded problems were from a) an employee and b) from a temporary worker assigned to Vitals. Changes to policies and procedures have addressed weaknesses related to those two events.

In light of the above, we do not agree that a documentable weakness exists that warrants the action recommended. A funds request to build added doors would not provide a benefit that justified the expense.

- 4.) *We concurred with the audit comment on this point in last year's recommendation, and we created procedures to address the recommendation. After the formal response was presented, nothing further was heard to suggest there was an issue with the response. The Vital Statistics Branch's current procedures remain the same as what was outlined in the corrective action response last year. The Department for Public Health feels that with the implementation of the new accounting system that was referred to in several audit responses that the new system will reduce problems and alleviate risks by having online tracking of data entry. The new accounting system should be implemented prior to January 2003.*

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS2: The Vital Statistics Branch Should Improve Controls Over
Assets And Separate Work Tasks (Continued)**

Management's Response and Corrective Action Plan (Continued)

- 5.) *Concur. Effective October 2002, the Accountant I is responsible to receive and enter the money received from funeral homes for pre-paid vouchers into the system. The Fee Control Unit Supervisor will then prepare vouchers to be issued to the funeral homes. She will also be responsible for tracking the vouchers as they are returned to Vital Statistics. Back ups will be assigned in the case of absences.*
- 6.) *The Vital Statistics Office is a customer service agency and must remain open to customers until 4:30 PM daily. The deposit is kept overnight in the office safe. The report is then reconciled the following day. With the present accounting system it is necessary to have the receipts at hand in order to reconcile the daily reports. This reconciliation can take several hours, sometimes until 2:00 or 3:00 that afternoon. The procedure of then holding the deposit until the following morning has been discussed with the Financial Management and Reporting Branch (FMRB) and Vital Statistics will begin taking the deposit up to FMRB in the afternoon of reconciliation if prior to 3:30 PM. The new accounting system should alleviate this problem.*
- 7.) *We concur. Effective June 18, 2002 (day after auditors' visit), the lateral file containing faxes requesting certified copies of certificates, credit card numbers, and expiration dates has been kept locked at all times except when a Vital Chek operator has needed information from the file. The faxes are disposed of every 60 days. As of October 16, 2002 the credit card number and expiration date is being redacted the day the fax is received.*
- 8.) *Concur – this item is open. We agree that there are acceptable risks when one employee performs multiple duties. It is a near impossibility to separate these duties using the present Virtual Address Extension (VAX) old accounting system and with the implementation of the new accounting program (in the new Vital Statistics Information System (VSIS)) this problem should be alleviated. A daily computerized report will be run by each data entry operator. With the edits and balances that have been built into the system, it is the goal of the system to prevent data operators from having an unbalanced daily report, therefore there would be no unbalanced reports for the Accountant III to reconcile. Of course, this will be after the operators become familiar with the system.*

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-CHS2: The Vital Statistics Branch Should Improve Controls Over Assets And Separate Work Tasks (Continued)

Management's Response and Corrective Action Plan (Continued)

Until that time the Accountant I will count the daily deposit prior to the Accountant III reconciling the daily report and then again count the deposit after the Acct. III has finished the reconciliation. As mentioned previously, the new system should be implemented prior to January 2003. Point of reference – the Accountant III has a list of operator ID's that is presently needed when reconciling reports, but she does not have access to each operator's password.

- 9.) *Prior to October 7, 2002 the front desk gave a receipt to any customer who requested it. As of October 7, cash register generated receipts are handed to all walk-in front desk customers. Since August 2002 the daily cash register tapes have been batched and reconciled to each operator's cash register reconciliation sheet.*

- 10.) *We agree that the safe should not be left open any longer than necessary and cannot be left unattended. This safe is in the direct view of the Section Supervisor's Office (within 10 feet), and also can be seen from two Office Supervisor's desks. All three are responsible for logging the safety paper in and out of the safe to the units. The safe was placed in this position to deter unauthorized staff from entering it. Effective October 2002 when logging security paper in and out, the supervisor who opens the safe is responsible for locking it immediately after removing or replacing security paper except in the case of a positive handoff to another supervisor.*

- 11.) *We were very general with our response to the 2001 related audit comment and have been following that response but effective October 2, 2002 logs are being kept in the safe for all checks issued on the Vital Chek Company. It is the responsibility of the Administrative Section Supervisor to keep the logs. Back ups have been assigned in the event of her absence (Fee Control Unit Supervisor, Accountant III, Accountant I). One log contains the date the blank checks are received from the Vital Chek Company, the number of checks received, the tracking numbers received and the signature of the Vital Statistics receiver. The second log (operator log) contains the date the operator received the check, the tracking number, on the check, and initials. Random weekly counting of remaining checks will take place. This process will show that the Vital Statistics office is striving for reasonable accountability of these checks. Since these checks already state, in red, that they are payable to "Deposit Only - Vital Records", it would be extremely hard to modify the check and then be used for personal gain.*

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-3: The Vital Statistics Branch Should Take Appropriate Steps To
Reduce The Identity Theft Risks**

The Vital Statistics Branch collects and registers data relating to Kentucky births, deaths, marriages, adoptions, and divorces. We observed the branch to follow-up on prior year audit findings.

Kentucky birth and death certificates are easy to obtain fraudulently and can be used for fraudulent purposes, such as identity theft. Identity theft could be facilitated by the ease with which vital records can be obtained.

Proper internal control dictates the Vital Statistics Branch not release:

- Data which is excluded by law and
- Data which could easily facilitate identity theft or other crimes.

Kentucky is one (1) of 13 states with “open” birth records and one (1) of 19 states with “open” death records. These open records states are far less restrictive on which records are exempted from disclosure and inspection.

KRS 61.878(1) excludes some public records from disclosure under the Open Records Law. This is specifically discussed in KRS 61.878(1)(a) and (l).

When KRS 213.011(14) and KRS 213.131(1) are read together, it is clear that vital records should not be open for inspection, except where specifically authorized. KRS 213.131(1) further states “administrative regulations adopted by the cabinet shall provide for adequate standards of security and confidentiality of vital records. . .” 901 Kentucky Administrative Regulation (KAR) Chapter 5 addresses vital statistics, but these regulations do not address adequate standards of security and confidentiality of vital records.

CHS responded to a similar comment in the prior audit and referred to OAG 81-400 and OAG 82-234 as support for the requirement that it disclose “open” birth and death records. The statutes noted above were amended several years after these Attorney General’s Opinions were issued. Identity theft did not become a serious problem until after 1996.

Proper internal control dictates that the branch not release data that is excluded by law, or data which might be likely to facilitate identity theft or other crimes.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-3: The Vital Statistics Branch Should Take Appropriate Steps To
Reduce The Identity Theft Risks (Continued)**

Recommendation

We recommend:

- The branch promulgate administrative regulations as required by KRS 213.131(1) to provide adequate standards of security and confidentiality of vital records.
- The branch take appropriate steps, including requesting legislation to exclude this data from potential misuse by persons seeking to commit identity theft or other unlawful acts. The end result should exclude any data that has the potential to be misused by persons seeking to commit identity theft or other unlawful acts.
- The branch should exclude social security numbers from death certificates subject to inspection under the Open Records law. The social security number on a death certificate released to the public should be excluded until such time as identity theft no longer appears to be a substantial risk.

Management's Response and Corrective Action Plan

This audit issue is a Commonwealth policy issue under discussion in Legislative committees. The Cabinet for Health Services, the Transportation Cabinet, the Attorney General's Office and the Office for Security Coordination are working together to create appropriate legislation that will tighten security and the open access of records, aid in the prevention of identity theft, and also make penalties stronger. This item should be closed.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-CHS-4: The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized

The Cabinet for Health Services (CHS) did not restrict critical information divulged by its network servers. During examination of the CHS local area networks (LANs) security for fiscal year 2002, we discovered several instances in which servers within the LANs provided information that could potentially assist an intruder in developing an approach to attack the system.

Using standard scanning tools we examined all computer device names and other remarks located within five CHS domains. The naming convention of servers was not sufficiently ambiguous to disguise the function of several computer devices. Further, remarks available from two computer devices might catch an intruder's interest.

We also ran other vulnerability assessment tools during fiscal year 2002 on forty-nine (49) servers within the CHS domains to determine if information was returned for Local Security Authority (LSA), Password Policies, Valid User, Group, or Share Lists. The table below depicts the number of servers that would provide this information.

Type of Information	Number of machines providing information	Percentage of 49 machines providing information
LSA	26	53%
Password Policies	46	94%
Valid User List	41	84%
Valid Group List	41	84%
Valid Share List	37	75%

Further, we found one server with port 2301 open. We were allowed to logon to the Compaq Insight Manager (CIM) application on this server with the default administrator userid and password. Access to the application provided excessive information to an unauthorized individual seeking knowledge of the system.

Finally, on five servers the PORTMAPPER service was running on port 111. We were given information about the system without providing a logon. This service supplies excessive information to a potentially unauthorized individual.

For security purposes, detailed server and user account information contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-4: The Cabinet For Health Services Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized (Continued)**

To help ensure the security surrounding an agency's domain information, agencies should ensure that information such as server location, accounts associated with the server, data residing on the server, and the server's role is not accessible to the public. To accomplish this, an agency should configure devices to not respond to certain types of inquiries, use naming conventions that obscure the purpose of servers, provide no comments on server activity, and restrict access to default logons for applications.

Recommendation

We recommend that CHS restrict the information provided by its LAN computer devices to anonymous users. First, the naming convention for servers should be altered to make them more ambiguous and any unnecessary computer device comments should be removed. Second, limitations should be placed on the type of response servers provide to system inquiries. Third, the default logons for the CIM application should be changed. Finally, access to the PORTMAPPER service should be restricted to authorized users.

Management's Response and Corrective Action Plan

CHS concurs with the recommendation by the APA and began updating its network servers to restrict access to Local Security Authority (LSA), Password Policies, Valid User, Group, and Share Lists in December 2002. Completion of these updates is estimated to be February 2003.

During 2002 DTR established ambiguous names for any newly installed servers. A plan to update existing naming conventions for every CHS server is being reviewed and a recommendation relating to an action plan will be made to CHS in March 2003.

With regard to the Compaq Insight Manager (CIM) login, the logon for the CIM application was updated in September 2002

In regard access to the PORTMAPPER service, this service remains on a single domain for CHS and a directive has been provided to the controlling agency to restrict this service to authorized users. A compliance date for this request has been set for February 2003 and an audit of this domain is scheduled to be conducted by DTR in March 2003.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-CHS-5: The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose

During our interim security vulnerability assessment testing for servers controlled by the Cabinet for Health Services (CHS), we found several CHS servers with ports open that may not have a specific business-related purpose. Due to the large number of issues, the findings are grouped below by port number and application.

Port 7 – Echo and Port 19 - Chargen

Five (5) servers had both ports 7 and 19 open. These ports are not necessary for the function of the server and could potentially be used to perpetuate a Denial of Service (DoS) attack.

Port 80 – Hypertext Transfer Protocol (HTTP)

First, port 80 was open on two machines but would not display the website. When no default page or restricted logon is required, normally this means that no application/web service is running at the port. Second, configuration information for printers or print servers was provided by ten websites and two servers appear to contain configuration information for switches. This situation allows too much access to an unauthorized or anonymous user. Third, there were eight servers provided web sites noted as the default or were under construction. There have been vulnerabilities documented with default installations of many HTTP services. Therefore, access to the World Wide Web should be restricted for any new HTTP installations until all applicable patches and security features have been implemented.

Port 443 – Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)

Ten (10) servers were found with port 443 open but would not display a website. When no default page or restricted logon is required, normally this means that no application/web service is running at the port.

Port 6667 – Internet Relay Chat

Eight (8) servers were discovered with port 6667 open. This port can be used for several serious exploitations such as DoS attacks, Trojan horse attacks, and downloading of illegal files. This port could be useful to a hacker and should only be used for a necessary business-related application.

Port 8000 – HTTP

Two (2) servers were discovered that had port 8000 open. Both servers provided links to error, event, and HTTP information. This situation allows too much access to an unauthorized user.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-5: The Cabinet For Health Services Should Ensure That All Open Ports On Agency Servers Have A Business-Related Purpose (Continued)**

Port 8080 – HTTP

Two (2) servers were discovered that had port 8080 open. Both servers provided links to error, event, and HTTP information. This situation allows too much access to an unauthorized user.

Other Ports

Ten (10) servers had ports open that do not appear to specifically relate to known business applications. Workforce should review all open ports on servers to ensure that all have a valid business-related purpose.

For security purposes, detailed server and user account information contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

The existence of open ports is an invitation for intruders to enter your system. Best practices dictates that only necessary, business-related ports should be open. Further, all applications residing at these ports should be secured to the extent possible.

Recommendation

We recommend that CHS perform a review of all open ports on the servers discussed in this comment. If there is not a specific business-related purpose requiring a port to be open, then that port should be closed. Further, we recommend that CHS begin a periodic review of open ports on all machines owned by the agency to ensure necessity.

Management's Response and Corrective Action Plan

Effective September 2002, DTR initiated actions to close any port that was not necessary for business-related activities of the Cabinet, including directives to all domains for compliance by February 2003. A follow up audit of all open ports is scheduled for April 2003. In addition, other procedures are scheduled to be implemented in March 2003 relating to review of open ports for newly installed application servers or software applications.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-CHS-6: The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers

As was noted in the prior audit, password policies established on certain critical Cabinet for Health Services (CHS) servers did not adhere to the agency password policies. During the FY 2002 audit, testing was performed to determine the accessibility of the password policies of all Primary Domain Controllers (PDC), Backup Domain Controllers (BDC), Structured Query Language (SQL), and a sample of Network (NT) servers within the five CHS domains using a vulnerability assessment tool. Of the forty-nine (49) servers tested, we were able to obtain the password policies for 46, or 93.9 percent, of these servers.

Password policies established on several servers within the five (5) CHS domains did not agree to the recommended password policy. See table below for findings.

Security Measure	Security Policy or Industry Standards	Number of machines not in compliance with policy	Percentage of 46 machines not in compliance with policy
Maximum Age	31 days	16 – 45 days 19 – 42 days 5 – None	87%
Minimum Age	1 day	25 – None	54%
Minimum Length	8 characters	20 – None	43%
Lockout Threshold	3 attempts	24 – None	52%
Lockout Duration	“Forever”	24 – 30 minutes 4 – 1,440 minutes	61%
Lockout Reset	1,440 minutes	26 – 30 minutes	56%

NetBIOS information was received from the 33 servers and was examined to determine if accounts adhered to the policy. We found user, guest, and/or administrator accounts on eleven (11) servers, or 33.3 percent of servers tested, which had been used to log onto the system but did not comply with the standard to change an account password at least every thirty-one (31) days.

For security purposes, detailed server and user account information contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated in writing to the appropriate agency personnel.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-6: The Cabinet For Health Services Password Policy Should Be Consistently Applied To All Local Area Network Servers (Continued)**

Passwords are a significant feature to guard against unauthorized system access. The failure to follow adequate password policy standards when establishing a system password could ultimately compromise the entire network. The purpose of a password policy is to establish a standard to create strong passwords, to protect those passwords, and to ensure passwords are changed within a specified time period. To assist in the security of a network, it is necessary for a strong policy to be developed and consistently implemented on all servers throughout the network.

Recommendation

We recommend that CHS review all servers within its agency-owned domains to ensure that the password policy established on all servers complies with the guidelines specified by the agency. Further, CHS should review its security policy to ensure that all applicable password policies are included and all user accounts comply with established policies. The security policy should be issued to all employees.

Management's Response and Corrective Action Plan

CHS concurs with recommendation of the APA. Effective April 2002, CHS directed that all computer password expire after 30 days, with the exception of those for domains for local health department (LHD's) which are to required to expire after 45 days in accordance with current agreements between the Department for Public Health and the LHD's.

Policies and procedures have been established regarding the validation and security of updating passwords. Strong passwords are enforced through network controls.

During 2003, DTR will increase its efforts to educate CHS staff through its newsletter, executive staff, and other communications regarding security and identification of passwords.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-7: The Cabinet For Health Services Should Remove The Simple Network Management Protocol Service Or Change The Default Community String**

During our interim vulnerability assessment testing of certain servers within the Cabinet for Health Services (CHS), the auditor found six servers having the Simple Network Management Protocol (SNMP) service available. This situation allows an anonymous user to logon with the community name “public”. The “public” community name is the default public account for this service. The use of the “public” community name allows excessive information to be provided to any anonymous user, such as listening ports, open sessions, active user accounts, and shares that exist.

For security purposes, detailed information concerning the specific servers that contributed to these findings is being intentionally omitted from this comment. However, complete detailed information is being provided to the responsible agency personnel in a separate transmission to assist them in addressing these issues.

Information provided by the SNMP service concerning a machine’s functions could be useful to an intruder in developing an attack. Access to the world at large through default logons should not be allowed.

Recommendation

We recommend that CHS either disconnect the SNMP service or change the “public” community name to a more sophisticated name on all servers. Further, any new machines should be checked for the SNMP service to ensure the “public” community name has been changed.

Management’s Response and Corrective Action Plan

CHS concurs with the recommendation of the APA, and effective December 2002, CHS servers were updated to change the “public” community name. A procedure is scheduled for implementation in March 2003 regarding review of SNMP services for newly installed machines, which will augment the present CHS policy governing the installation of applications on the CHS network.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-CHS-8: The Cabinet For Health Services Should Ensure All User Accounts On Its Agency Servers Are Necessary

While performing interim vulnerability tests of the Cabinet for Health Services (CHS), we found several instances where it appears unnecessary accounts were established on servers or for applications.

To examine the information provided by NetBIOS, we tested a sample of forty-nine (49) machines within five CHS domains, including the Primary Domain Controller (PDC), Backup Domain Controllers (BDC), SQL servers, and NT servers. NetBIOS account information was obtained from thirty-three (33) servers, including two (2) PDCs, twelve (12) BDCs, nine (9) SQL, and ten (10) NT servers. When examining this information we found that there were disabled accounts on sixteen (16) servers and accounts that had never been used on fifteen (15) servers. Further, there were accounts on eleven (11) servers that had logged on in the past but whose password age was over the expected thirty-one (31) days.

The auditor attempted a remote logon to known applications using various combinations of default logon passwords. A review of machines controlled by CHS revealed thirty-two (32) machines with port 21 open and seventy-one (71) machines with port 23 open. We were able to create a File Transfer Protocol (FTP) session through port 21 on eighteen (18) machines, 56 percent, using the anonymous login. In addition, Telnet sessions could be established with no login or through the anonymous default login on ten (10) machines, or 14 percent, through port 23.

For security purposes, detailed server or user account information contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Intruders often use inactive accounts to break into a network. If a user account has not been used for a period of time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will use the account. An account should be deleted if it is not going to be reinstated. Further, default Administrator, Guest, and Anonymous accounts in operating system and applications are among the initial accounts that an intruder will attempt to use. Therefore, they should be assigned strong passwords or, if possible, renamed or removed immediately after installation.

Recommendation

We recommend that CHS review accounts on all servers to determine which accounts had no password change within the last thirty-one (31) days. These accounts should be evaluated to determine if they are still valid accounts required for a business-related purpose. If not, the accounts should be disabled or deleted.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-8: The Cabinet For Health Services Should Ensure All User
Accounts On Its Agency Servers Are Necessary (Continued)**

Recommendation (Continued)

as appropriate. Further, Finance should ensure that all machines with FTP or Telnet services running on them restrict access to default, anonymous, or guest logons.

Management's Response and Corrective Action Plan

CHS concurs with the recommendation by the APA and effective September 2002, updated its procedure relating to the identification and removal of inactive users from the network. Prior processes inactivated accounts, which were reestablished for replacement personnel.

CHS anticipates implementing an internal exit procedure effective April 2003 for employees, contractors and temporary staff to assure that network access is terminated as early as possible.

CHS has removed one FTP server from service, whereas, other systems with open ports or Telnet services have been determined to be either printers or necessary for business operations.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-9: The Vital Statistics Branch Has An Outdated Computer System**

The Vital Statistics Branch has a stand-alone system that is used for handling receipts and issuing various certificates. This system has been in place since 1983 and is extremely outdated, which increases the risk of operational problems with the programs or a failure of the entire system.

If the system fails for any reason, no certificates could be recorded or issued via the existing computer system. Due to the outdated system in use, there is a risk of prolonged downtime.

Proper internal control requires an agency to maintain and safeguard its assets, which in this case are the vital statistics of the people of Kentucky. The computer hardware and software should be adequate to meet the normal operational business needs of the Vital Statistics Branch.

Recommendation

We recommend the Vital Statistics Branch update the computer system that records the vital statistics and issues the certificates of those statistics in order to assure that this data is always available in a timely manner. Manual procedures should be documented in the event that the branch would have to return to manual procedures.

Since there appears to be a real risk that the old system may stop functioning before it is replaced with a new system, the branch should explore various interim approaches that could be used to improve the workflow and speed-up the recovery time. For example, the branch may be able to use PCs and some software with blank forms to capture data, facilitate the workflow, and enable batch loading of data to speed the recovery time.

Management's Response and Corrective Action Plan

This item remains open. As mentioned in several 2001 RCW responses, Vital Statistics was in the process of hiring a vendor to create an electronic Vital Statistics Information System. The Commonwealth has invested \$2,000,000 in this project and a contract was let with a vendor in June 2002. The vendor and many Vital Statistics staff have been working diligently in designing a new accounting system with minimum risks. If everything stays on track, with no major problems arising, the new accounting system is projected to go online prior to January 2003.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 02-CHS-10: Vital Statistics Policies And Procedures Should Be Upgraded

The Vital Statistics Branch is in the Kentucky Department for Public Health, which is within the Cabinet for Health Services. The Branch's employees consist of data entry clerks, accountants, telephone operators, and cash register clerks.

In FY 2001, the branch updated their policies and procedures manual to cover most areas of work. The manual does not cover weaknesses that were found while conducting the audit. We noted problems in the following areas:

- 1) The signed blank checks being accounted for in a log book two to three times a week,
- 2) Fax orders being stored in a locked file cabinet at all times,
- 3) Mail distribution is not to be performed by data entry clerks,
- 4) Receipts to be issued to all walk-in requests,
- 5) Cash register clerks should reconcile end of day receipts to the cash register tape at the end of every day,
- 6) The prepaid vouchers should be distributed by a different Branch employee than the one collecting the fees,
- 7) The Accountant III should not perform the end of day reconciliation and deposit preparation,
- 8) The certificate safe should be locked at all times except short periods to place items into the safe or remove items from the safe,
- 9) Voided certificates should be kept for a reasonable period of time,
- 10) Branch receipts should be secure at all times,
- 11) Receipts should be deposited at the earliest possible time, and
- 12) The branch should create process guidelines for when key personnel are absent

Without a complete policies and procedures manual in place, the Branch's employees do not have a full description of their duties. This can cause possible control weaknesses. A complete policies and procedures manual will provide a structure for the Branch's employee duties.

Recommendation

We recommend the Branch's policies and procedures manual be updated to cover the weaknesses found while conducting the audit.

Management's Response and Corrective Action Plan

The Vital Statistics' Office Procedures Guide is continually being updated. Written procedures concerning weaknesses addressed in the 2002 RCW's will be updated on implementation of changes made to cover each weakness.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-11: The Timesheet Preparation Process Needs Better Oversight**

As part of our payroll and personnel audit, internal control testing was performed over timesheets. We randomly selected 45 timesheets for our sample.

We noted seven (7) different timesheets with exceptions to our test attributes. These exceptions include:

1. Mathematically Incorrect (1)
2. Employee's signature missing (1)
3. Supervisory signature missing (1)
4. Supervisor's signature card not on file (4)

Failure to properly review timesheets may result in incorrect payroll charges. These problems may result in improper payments or benefits to employees, and excessive payroll charges to the Commonwealth.

Effective internal control dictates that timesheets are signed by every employee and supervisor to ensure that all submitted timesheets are correct and authorized.

Recommendation

We recommend the following:

- All timesheets need the employee's signature;
- All timesheets should be reviewed for accuracy and completeness by the supervisor, whose signature indicates correctness;
- All leave time should be approved in advance or as required by agency policy;
- All supervisors must have signature cards on file

Management's Response and Corrective Action Plan

The Cabinet is in the process of identifying all supervisors responsible for signing and ensure signature cards are on file, as well as reiterate the requirement to have leave time approved in advance and have signatures and correct totals on the time sheets. Cabinet also will ensure that all staff specifically responsible for re-checking time totals are in place and properly performing this duty.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-12: The Division Of Program Integrity Has A Large
Outstanding Balance Of Accounts Receivable For The Drug Rebate Program**

State Agency: Cabinet for Health Services

Federal Program: CFDA 93.778 – Medical Assistance Program

Federal Agency: U.S. Department of Health and Human Services

Pass-Through Entity: Not Applicable

Compliance Area: Allowable Costs/Cost Principles

Amount of Questioned Costs: None

Historically, the Division of Program Integrity has not actively sought payment on accounts receivable aged over 60 days. The division sends a notice to delinquent drug manufacturers after 38 days. Another notice is sent after 60 days to request payment or reason for amount disputed. After the second notice is sent there are not any other formal attempts at settlement. The current director and his staff have been more active but there still remains a large amount of accounts receivable outstanding.

There have been several attempts to collect outstanding amounts. Healthfirst has been contracted to collect claims for 1999 and 2000. At the end of their contract, depending on their success, they will be re-hired to collect 1991- 1998. Also, one (1) employee was sent to the Dispute Resolution Program, sponsored by the federal department of Health and Human Services, to learn more about solving aged disputes. Further, DHHS, Office of Inspector General will also be performing audits in 49 of the 50 states, including Kentucky, to determine how to improve drug rebate procedures.

As of June 30, 2002, accounts receivable balance for the Drug Rebate program was \$44,573,000. The uncollected portion for FY 02 is \$5,674,000. Medicaid is potentially losing millions of dollars that could help offset budget deficits in the coming and present fiscal year.

The Medicaid Drug Rebate Program, created by the Omnibus Budget Reconciliation Act (OBRA) of 1990 states the following:

Except as provided under V(b), to make such rebate payments for each calendar quarter within 30 days after receiving from the State the Medicaid Utilization Information defined in this agreement. Although a specific amount of information has been defined in I(n) of this agreement, the Manufacturer is responsible for timely payment of the rebate within 30 days of receiving, at a minimum, information on the number of units paid, by NDC number. In the event that in any

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-12: The Division Of Program Integrity Has A Large
Outstanding Balance Of Accounts Receivable For The Drug Rebate Program
(Continued)**

quarter a discrepancy in Medicaid Utilization Information is discovered by the Manufacturer, which the Manufacturer and the State in good faith are unable to resolve, the Manufacturer will provide written notice of the discrepancy, by NDC number, to the State Medicaid Agency prior to the due date in II(b). If the Manufacturer in good faith believes the State Medicaid Agency's Medicaid Utilization Information is erroneous, the Manufacturer shall pay the State Medicaid Agency that portion of the rebate amount claimed which is not disputed within the required due date in II (b).

In addition, proper accounting procedures for accounts receivables require balances be monitored and immediate action taken for outstanding balances.

Recommendation

We believe the new director and his staff are improving efforts for monitoring accounts receivable and implementing new procedures in an attempt to correct years of oversight. We recommend the accounts receivable balance continue to be monitored and collection procedures continue to be pursued.

Management's Response and Corrective Action Plan

The Department for Medicaid Services concurs with the recommendation and will continue to monitor as well as pursue accounts receivable collections. Additionally, DMS will strive to enhance current collection procedures.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-13: The Division Of Program Integrity Does Not Track Interest Due On Outstanding Drug Rebate Accounts**

State Agency: Cabinet for Health Services

Federal Program: CFDA 93.778 – Medical Assistance Program

Federal Agency: U.S. Department of Health and Human Services

Pass-Through Entity: Not Applicable

Compliance Area: Allowable Costs/Cost Principles

Amount of Questioned Costs: None

The Division of Program Integrity (Program Integrity) does not track interest due on outstanding balances for the Drug Rebate Program. As part of our testing for collections, as required by the Compliance Supplement, we noted 47 of the 100 manufacturers tested had interest due. Forty manufacturers did not pay any interest. Of the seven that paid, there was not any evidence the agency verified the amount paid was reasonable. The auditors inquired how interest was computed on outstanding balances. The agency explained the manufacturers computed it. No one in the agency recomputed to determine the amount paid was appropriate. DMS has the responsibility to track the amount of interest due from each manufacturer. The director and manager have been made aware of this problem and are trying to have the interest due calculated automatically, so a comparison can be made when payments are received.

The Medicaid Drug Rebate Program, created by the Omnibus Budget Reconciliation Act (OBRA) of 1990 states:

The balance due, if any, plus a reasonable rate of interest as set forth in section 1903(d)(5) of the Act, will be paid or credited by the Manufacturer or the State by the due date of the next quarterly payment in II(b) after resolution of the dispute.

Since Program Integrity is not tracking interest, the state could be losing several thousand dollars to offset the federal match. Drug manufacturers are responsible for calculating and paying the proper interest rates. However, this does not relieve DMS of the responsibility of control over this area and know which manufacturers should be paying interest and how much interest they should be receiving.

Government entities should maintain control over accounts receivables as stewards of public funds. Allowing companies to calculate and pay interest with no checks or oversight allows for discrepancies and is a lack of control.

FINANCIAL STATEMENT FINDINGS

***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance***

**FINDING 02-CHS-13: The Division Of Program Integrity Does Not Track Interest
Due On Outstanding Drug Rebate Accounts (Continued)**

Recommendation

We recommend the Division of Program Integrity calculate and track interest due on outstanding balances so comparisons can be made to manufacturers payments and any discrepancies corrected.

Management's Response and Corrective Action Plan

Program Integrity is currently working to redesign the system to calculate and track the interest on outstanding accounts, and we anticipate our system will be sufficiently programmed and tested for this function between July 1 and August 1, 2003.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-14: The Division Of Managed Care Does Not Maintain Records Of Complaints And Grievances**

State Agency: Cabinet for Health Services

Federal Program: CFDA 93.778 – Medical Assistance Program

Federal Agency: U.S. Department of Health and Human Services

Pass-Through Entity: Not Applicable

Compliance Area: Special Test and Provisions

Amount of Questioned Costs: None

For three (3) years we have performed testing of internal controls and compliance of the Complaint/Grievance Call Log System. Each year we continue to find cases in our testing that complete information is not being entered in the system. Each year CHS has stated in their corrective action plan a new system was being implemented. In response to the comment for FY 01 the Management and Corrective Action Plan stated the following:

The Department for Medicaid Services is in the process of moving to a new technology by going to a client server environment that will be used to develop and implement the Health Insurance Portability and Accountability Act (HIPPA) requirements. {The QCSI-based (QCSI is Quality Care Solutions, Inc., which is a health care software vendor. See <http://www.qcsi.com>) solution has features the current Medicaid Management Information System (MMIS) does not have (e.g., an integrated call tracking feature).} Each call will be logged based on time of call, user ID (person entering information into the system) and will be linked to the provider number (if the provider is enrolled into the Medicaid program) and/or to the member's Medical Assistance Identification (MAID) number. If the caller is provider/member not enrolled in the Medicaid program the call will be logged by name.

When the APA requested access to the complaint log, the auditor was told that the complaints were documented on paper forms. After the call was routed to the proper division the form was not saved due to lack of storage space. Thus, the auditor could not perform tests in this area.

The Complaint/Grievance system cannot be used to it's full potential by agency personnel unless all data is entered into the system. For FY 02 there is not any evidence the complaint/grievance system was used. Therefore, Medicaid providers and recipients problems may go unresolved. Unresolved problems could lead to endangerment of Kentuckians or fraud not being examined.

A government entity needs an internal control structure that provides a way to ensure compliance with laws and regulations. The complaint/grievance log is intended to ensure providers and recipients their problems are examined.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 02-CHS-14: The Division Of Managed Care Does Not Maintain Records
Of Complaints And Grievances (Continued)**

Recommendation

We recommend the agency follow through with its corrective action plan from 2001. If this cannot be done then a complaint/grievance log system should be implemented that can be tracked and tested. This will ensure agency personnel have all relevant data to make determinations on how to resolve a complaint/grievance.

Management's Response and Corrective Action Plan

The Department for Medicaid Services currently operates a toll-free number for Medicaid recipients to request assistance with problems and concerns they have regarding the Medicaid program. This is not a provider assistance line. Providers are assisted through a separate provider relations line with our fiscal agent. Medicaid does utilize a call tracking system that tracks the number of calls, how long it takes to answer a call, which Representative took the call, how long the call lasts, how many calls are lost and gives recipients the opportunity to leave a message if their call is not answered timely.

Beginning in January 2003, the Medicaid Member Services Branch implemented a temporary electronic tracking system using Excel Spreadsheets. Calls are logged as they come in. For each phone call, the Member Service Representative logs the caller's name and phone number, the recipient's name and Medicaid ID number, a description of the problem/issue, the resolution, and to whom the call was transferred. The spreadsheets are collected electronically at the end of each day and filed in electronic folders. This is a temporary system until Medicaid implements a new call tracking system on June 1, 2003. The new system will be capable of collecting the information mentioned above and will electronically link the recipient call to the Representatives and allow the Representatives and supervisors to electronically track cases until they are closed. The new system will also allow Representatives to access other information pertinent to the recipient.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Compliance*****FINDING 02-CHS-15: The Division Of Systems And Member Services Does Not Reconcile Supplementary Insurance Billing**

State Agency: Cabinet for Health Services

Federal Program: CFDA 93.778 – Medical Assistance Program

Federal Agency: U.S. Department of Health and Human Services

Pass-Through Entity: Not Applicable

Compliance Area: Activities Allowed or Unallowed

Amount of Questioned Costs: None

The Division of Systems and Member Services, does not reconcile information for the Kentucky Supplementary Medical Insurance (SMI) program between Unisys and billing notices from Center of Medicare and Medicaid Services (CMS) reports to ensure valid claims have been properly processed; therefore, assuring CHS is not over paying.

Agency procedures indicate, on the 25th of each month, or the next business day, Unisys prepares a report of monthly SMI transactions. This report is sent to the Department of Social Insurance (DSI) for corrections then to CMS for comparison to its database. CMS then prepares a bill and sends it to CHS.

When CHS receives the bill from CMS a comparison is made to the original Unisys report. The purpose of this reconciliation is to verify valid claims have been properly processed and properly recorded.

The manager for SMI informed us the reports have been reconciled for fiscal year 2003. The manager for SMI produced reconciled reports for FY 03. APA personnel observed the reports. Further testing will be done in the FY 03 audit.

Due to the lack of reconciliations for the State may be over paying for SMI costing the State additional funds that are needed to balance the Medicaid budget.

A government entity needs an internal control structure which provides controls to ensure compliance with laws regulations, safeguards it's assets, checks the accuracy and reliability of it's accounting data, and promotes operational efficiency. A good internal control structure is essential for accountability, which is the prime issue in today's government.

Recommendation

We recommend Medicaid continue to reconcile the reports and make corrections when discrepancies are found.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Compliance*****FINDING 02-CHS-15: The Division Of Systems And Member Services Does Not Reconcile Supplementary Insurance Billing (Continued)**

Management's Response and Corrective Action Plan

The Department for Medicaid Services Systems and Member Services Division and Unisys have made corrections to the monthly KYMQ1200 – R04 Buy-In Financial Summary Report. The report lists the amounts that DMS expects to be billed by CMS for Part A and Part B Buy-In recipients. Once DMS receives the CMS Billing Notice for Part A, Agency Code S18, (Branch Manager, Member Services) reconciles the billing balance to the KYMQ1200 – R04. If there are discrepancies, then the monthly KYMQ1230 – R01 Part A Bypassed Report is used to reconcile the difference. At this time, there have not been any discrepancies between the Billing Notices and the Q1200 – R04 for Part A. DMS also receives a Billing Notice for Part B, Agency Code 180. This is reconciled to the Q1200 – R04 for Part B. The KYMQ1230 – R02 Part B Bypassed Report, which displays the transactions Unisys bypassed from the CMS Buy-In transmission, is used to reconcile the difference. Since the KYMQ1230 – R02 was created in 8/02, DMS has been able to accurately account for the difference between the expected bill and the actual bill for Part B. The Member Services Branch uses the KYMQ1230 – R02 to update and correct the bypassed recipient records.

DMS will continue to utilize these reconciliation processes as recommended by the APA and will continue to explore for improvements in the reconciliation process.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Compliance

FINDING 02-CHS-16: The Office Of Aging Does Not Document The Performance Of Desk Reviews

State Agency: Cabinet for Health Services

Federal Program: CFDA 93.044 and 045 – Special Programs for the Aging – Title III, Parts B & C

Federal Agency: U.S. Department of Health and Human Services

Pass-Through Entity: Not Applicable

Compliance Area: Subrecipient Monitoring

Amount of Questioned Costs: None

The Office of Aging Services (OAS) did not document their performance of desk reviews of the Independent Auditor's Report submitted by Area Development Districts (ADD).

In order to effectively monitor subrecipients, Independent Auditor's Reports submitted by the subrecipient should be reviewed to determine whether the ADD had any reportable conditions or questioned costs related to applicable programs. Also, reports should be reviewed and compared for accuracy and completeness of grant funding information. Management cannot make informed decisions about frequency and intensity of monitoring and funding decisions without proper documentation of review of reports.

910 KAR 1:220 § 3 (10) (a) 7 states that OAS shall "Conduct monitoring through the review and analysis of reports submitted to the office by the area agencies on aging." While desk monitoring is evident on Area Plans and is supported by the Plan Review Checklist, there is no such support for desk monitoring of the Independent Auditor's reports submitted by the Area Agencies.

Recommendation

We recommend OAS staff conducting desk monitoring of reports submitted by the Area Agencies on Aging maintain documentation of such monitoring.

Management's Response and Corrective Action Plan

The Office of Aging Services currently performs a review of the Area Development District independent audits as far as they relate to funding for aging services and the personal care attendant program. The Office will develop a monitoring checklist, developed in part from the Standards of the President's Council on Integrity and Efficiency as it appears that this tool is generally used for a full desk review of all programs and of the qualifications of the auditor as well. We are also in the process of requesting copies of the full desk reviews for ADD's from the Department for Local Government and of the Title V providers from the CHS Office of Inspector General.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Compliance*****FINDING 02-CHS-17: The Office Of Aging Did Not Make Monitoring Visits To All Area Agencies**

State Agency: Cabinet for Health Services

Federal Program: CFDA 93.044 and 045 – Special Programs for the Aging – Title III, Parts B & C

Federal Agency: U.S. Department of Health and Human Services

Pass-Through Entity: Not Applicable

Compliance Area: Subrecipient Monitoring

Amount of Questioned Costs: None

The annual monitoring visit for Cumberland Valley Area Agency on Aging was conducted on July 24, 2002. This visit occurred following the close of State Fiscal Year 2002.

Without proper subrecipient monitoring, the Office of Aging Services cannot effectively detect deficiencies in performance of program requirements and activities of subrecipients.

910 KAR 1:220 § 3 (10) (a) 2 states that OAS shall “Conduct annual or more frequently, if indicated on-site monitoring visits to the area development districts.”

Recommendation

In order to effectively monitor subrecipients, OAS should conduct an on-site monitoring visit to each Area Agency on Aging during each fiscal year.

Management’s Response and Corrective Action Plan

It is always the practice of the Office of Aging Services to conduct annual monitoring of the Area Agencies on Aging prior to the end of each fiscal year. Due to staff vacancies, an isolated instance of inability to conduct the monitoring prior to the end of state fiscal year 2002 occurred. Therefore, it was necessary to conduct the SFY 2002 monitoring of the contract with the Cumberland Valley Area Development District in July, 2002.

Plan of Correction: The Office of Aging Services will schedule annual monitoring for each fiscal year prior to the end of the state fiscal year.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Reportable Conditions</u>					
<i>(1) Audit findings that have been fully corrected:</i>					
FY 01	01-CHS-2	The Department For Public Health Should Complete A Formal Information System Security Policy	N/A	N/A	New policy manuals issued and distributed during FY 02.
FY 01	01-CHS-3	The Financial Management and Reporting Branch Should Limit Access To Deposits			Resolved for FY 02.
FY 01	01-CHS-5	The Vital Statistics Branch Should Perform An Accurate Cash Reconciliation			Resolved for FY 02.
FY 01	01-CHS-10	The Cabinet For Health Services Should Reconcile The Supplementary Medical Insurance Data To The Agency Level Unisys Reports	93.778		Due to improvements, this finding is downgraded to an other matter for FY 02. This finding is no longer required to be reported under <i>Government Auditing Standards</i> . See 02-CHS-15
FY 01	01-CHS-11	The Division Of Substance Abuse Progress Reports For Subrecipient Monitoring Should Be Submitted In A Timely Manner	93.959		The agency has implemented sufficient subrecipient monitoring procedures to ensure compliance
FY 01	01-CHS-12	The Cabinet For Health Services Should Have A System To Identify Suspended Or Debarred Vendors	All		Procurement, Suspension and Debarment was tested at FAC, which maintains oversight for internal controls and compliance. Test results indicated the Commonwealth complied with this requirement for FY 02.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Reportable Conditions (Continued)</u>					
<i>(1) Audit findings that have been fully corrected (Continued):</i>					
FY 00	00-CHS-6	The Division of Substance Abuse Should Establish Procedures To Monitor Progress Reports	93.959		The agency has implemented sufficient subrecipient monitoring procedures to ensure compliance
FY 00	00-CHS-9	The Cabinet For Health Services Should Develop Procedures To Ensure Vendors Providing Services To Federal Programs Are Not Debarred Or Suspended By The Federal Government	All		Resolved for FY 02. See 01-CHS-12
FY 97	97-CHS-47	The Finance And Administration Cabinet And The Cabinet For Health Service Should Develop Procedures To Ensure Vendors Providing Services To Federal Programs Are Not Debarred Or Suspended By The Federal Government	All		Resolved for FY 02. See 01-CHS-12
FY 97	97-CHS-49	The Department For Public Health Should Develop A Complete Information System Security Policy	N/A	N/A	This comment was superseded in FY 01 by comment 01-CHS-2 referred to above.
<i>(2) Audit findings not corrected or partially corrected:</i>					
FY 01	01-CHS-4	The Vital Statistics Branch Should Improve Security Over Assets And Segregate Job Duties			Although progress has been made, there are still areas that need improvement. See 02-CHS-2
FY 01	01-CHS-6	The Vital Statistics Branch Should Take Steps To Prevent Identity Theft			The Cabinet For Health Services will seek legislation again. See 02-CHS-3.
FY 01	01-CHS-9	The Drug Rebate Program Should Be More Involved In The Dispute Resolution Program In Order To Collect More Money	93.778		There continues to be a large amount of Drug Rebate accounts receivable outstanding. See 02-CHS-12.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Reportable Conditions (Continued)</u>					
<i>(2) Audit findings not corrected or partially corrected (Continued):</i>					
FY 00	00-CHS-5	The Department For Medicaid Services Should Improve Claims Processing, Including The Dispute Resolution Process With Drug Rebate Manufacturers	93.778		There continues to be a large amount of Drug Rebate accounts receivable outstanding. See 02-CHS-12
FY 99	99-CHS-7	The Department For Medicaid Services Should Improved The Controls Over Drug Rebate Billings, Collections And Recordings.	93.778		There continues to be a large amount of Drug Rebate accounts receivable outstanding. See 02-CHS-12.
<i>(3) Corrective action taken is significantly different from corrective action previously reported:</i>					
There were no findings for this section.					
<i>(4) Audit finding is no longer valid or does not warrant further action:</i>					
FY 01	01-CHS-1	Custom Data Processing, Inc. Should Improve System Security Controls For Cabinet For Health Services Data	N/A	0	This issue was covered through the SAS 70 review.

Material Weaknesses/Noncompliances

(1) Audit findings that have been fully corrected:

There were no findings for this section.

(2) Audit findings not corrected or partially corrected:

There were no findings for this section.

(3) Corrective action taken is significantly different from corrective action previously reported:

There were no findings for this section.

(4) Audit finding is no longer valid or does not warrant further action:

There were no findings for this section.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2002

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Other Matters</u>					
<i>(1) Audit findings that have been fully corrected:</i>					
There were no findings for this section.					
<i>(2) Audit findings not corrected or partially corrected:</i>					
FY 01	01-CHS-7	Vital Statistics Should Update Its Computer System			CHS has made progress on this issue. The new system is expected to be in place by January 2003.
FY 01	01-CHS-8	Vital Statistics Should Update Its Policies And Procedures Manual			CHS has created a manual. This is an on-going process.
FY 00	00-CHS-10	The Department For Medicaid Services Should Strengthen Controls Over Supplementary Medical Insurance Bills	93.778		Medicaid still did not reconcile SMI bills for FY 02 but has begun doing it for FY 03. See 02-CHS-15
FY 99	99-CHS-12	The Department For Medicaid Services Should Strengthen Controls Over Supplementary Medical Insurance Bills	93.778		Medicaid still did not reconcile SMI bills for FY 02 but has begun doing it for FY 03. See 02-CHS-15
<i>(3) Corrective action taken is significantly different from corrective action previously reported:</i>					
FY 01	01-CHS-13	All Relevant Data Should Be Entered Into The Managed Care Program's Complaint/Grievance Call Log System In Order To Make Proper Determinations On How To Resolve A Complaint Or Grievance	93.778		Medicaid implemented a manual program while attempting to implement the corrective action plan. The manual plan did not provide any audit documentation. The system described in the corrective action plan never operated during the year. See 02-CHS-14
FY 99	99-CHS-11	Internal Controls Over The Managed Care Program Should Be Improved	93.778		See 01-CHS-13 above.
<i>(4) Audit finding is no longer valid or does not warrant further action:</i>					
FY 00	00-CHS-3	The Cabinet For Health Services Should Strengthen Controls Over Cash Receipts			These were upgraded to reportable in FY 01. See 01-CHS-3 and 01-CHS-4 in FY 01.

